REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

In addition, the Applicants' representative would like to thank Examiner Moorthy for kindly taking a substantial amount of time on April 5, 2006 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. STATUTORY DOUBLE PATENTING

The Examiner submits that claims 7 and 9 of the present Application conflict with claims 1 and 3 of co-pending, commonly assigned U.S. Patent Application Serial No. 09/944,788 (hereinafter "the '788 Application"). The Examiner requests that the allegedly conflicting claims be cancelled from either the present application or from the '788 Application, in accordance with 37 CFR §1.78(b). In response, the Applicants have cancelled claims 7 and 9 from the present application. Accordingly, the Applicants respectfully request that the statutory double patenting rejection be withdrawn.

II. REJECTION OF CLAIMS 1-2 AND 4-9 UNDER 35 U.S.C. § 102

1. Claims 1, 2, 4 and 5

Claims 1, 2, 4 and 5 stand rejected as being anticipated by the Baker patent (U.S. 6,775,657, issued November 19, 2002, hereinafter "Baker"). The Applicants respectfully traverse with the rejection.

Particularly, the Examiner's attention is directed to the fact that Baker fails to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, where the belief state indicates a state of a system resource or service and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claims 1, 4 and 5.

Baker does not teach, show or suggest sensors that maintain a belief state

indicating a state of a system resource or service (*e.g.*, normal, degraded, compromised, etc.). Furthermore, even assuming *in arguendo* that the sensors described by Baker could be considered to maintain "belief states", Baker does not teach, show or suggest that a given sensor's belief state may be shared with other sensors or modified based on the belief state of another sensor. In fact, nowhere does Baker teach or suggest that a sensor can communicate or share information with other sensors at all. Baker at most teaches that sensor data may be transmitted to one or more "directors" or centralized management consoles that compile sensor data (*i.e.*, not sensors). These directors do not maintain or update any sort of "belief" regarding the statuses of system resources, but merely collect data from sensors, translate the data and present the data for human analysis (*See, e.g.*, Baker at column 7, lines 35-41 and column 8, lines 17-22). Thus, data received from one sensor (collected by a director) is clearly not shared with other sensors. As sensor data is not shared among sensors, there can be no configuring of sensors based on information received other sensors, as suggested by the Examiner in the Advisory Action. Thus, Baker does not teach that sensors maintain belief states regarding the statuses of network resources or services, that a first sensor can transmit its belief state to a second sensor, or that the second sensor can modify its belief state based on the belief state received from the first sensor.

The Examiner alleges in the Advisory Action that "in neither claims 1, 2, 4 or 5 is it claimed that sensors maintain a belief state indicating a state of a system resource or service. The Applicants respectfully disagree and assert that such limitation is, in fact, clearly recited at least in claims 1, 4 and 5.

Claim 1, for example, recites "[a] method for correlating a first sensor and a second sensor ... the first and second sensors each maintaining belief over a number of possible states of the system" (claim 1, lines 1-3, emphasis added). Claim 1 goes on to recite that these belief states maintained by the first and second sensors "[indicate] a state of at least one system resource or service" (claim 1, line 5, and similarly at lines 6-7, emphasis added). Claim 4 similarly recites an "intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system" (claim 4, lines 2-4, emphasis added), where the maintained belief is in regards to "an apparent normal, degraded or compromised state of a monitored resource" (claim

4, line 6, and similarly at line 9, emphasis added). Claim 5 recites an "intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system" (claim 5, lines 2-4, emphasis added), where the maintained belief is in regards to "the existence or validity of services supported on monitored computer system resources" (claim 5, lines 5-7, and similarly at lines 8-9).

Thus, Applicants' invention clearly claims a method in which sensors maintain belief states regarding states of network resources or services and adjust these belief states based on at least part of another sensor's belief state, as recited by the Applicants in independent claims 1, 4 and 5. In their entireties, Applicants' claims 1, 4 and 5 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm. (Emphasis added)

5. A method for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources; and

(b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious.

(Emphasis added)

As discussed above, nowhere does Baker teach or even suggest the desirability of maintaining belief states at sensors regarding the statuses of network resources or services or adjusting the maintained belief state of a sensor, based on a belief state of another sensor. Therefore, the Applicants submit that independent claims 1, 4 and 5 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Baker. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

2. Claims 6-9

Claims 6-9 stand rejected as being anticipated by the Bristol patent (U.S. 6,690,274, issued February 10, 2004, hereinafter "Bristol"). In response, the Applicants have cancelled claims 6-9. Accordingly, the Applicants respectfully request that the rejection be withdrawn.

III. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Baker in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Baker and Timm, singularly or in any permissible combination, fail to disclose or suggest the novel invention of maintaining belief states at sensors in an intrusion detection system regarding the statuses of network resources or services, transmitting information about a second sensor's belief state to a first sensor or adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above.

As discussed above, nowhere does Baker teach or even suggest the desirability

of adjusting a belief state of a sensor relating to a state of a monitored system resource or service supported thereon, based on a belief state of another sensor. Timm does not bridge this gap in the teachings of Baker. Baker and Timm, singularly or in any permissible combination, thus fail to teach, suggest or make obvious a method in which a first sensor's belief state relating to a state of a network resource or service is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Baker in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

5/30/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702